Symantec AntiVirus Corporate Edition v9.0.3

Engineering Acceptance Document v1.1

for US Army NETCOM-ESTA

13 December, 2004

Accepted By:

Approval Signatures

DSE Primary – Greg Schoeneman ______________________________ Date __ / __ / __

DSE Peer Engineering – Anthony Bernardo ______________________________ Date __ / __ / __

Customer Primary – Cade King ______________________________ Date __ / __ / __

Customer Program Manager – Amy Harding ______________________________ Date __ / __ / __

Service Delivery[‡†] – N/A ______________________________ Date __ / __ / __

CSC Security[†] – N/A ______________________________ Date __ / __ / __

[‡] Required ONLY for EAD's containing items with rate based service indicators

[†] Required for any application that modifies the default security or as otherwise required by the account or customer

DISCLAIMER

The contents of this document and/or media are not to be construed as an official Department of the Army position unless so designated by other authorized documents. The use of trade names in this document and/or media does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement. Do not release to other than the intended recipient(s).

CHANGES

Refer requests for all changes that affect this document to: Director, NETCOM/ESTA, ATTN: NETC-EST-G, Fort Huachuca, AZ 85613-7070.

DISPOSITION INSTRUCTIONS

If this document/media is no longer required then it should be destroyed rather than returned to the issuing organization. Safeguard and/or destroy this document with consideration given to its classification or distribution statement requirements.

THIS IS A SENSITIVE BUT UNCLASSIFIED DOCUMENT.

Application Description

Taken from Symantec's website on 12/02/2004:

Symantec AntiVirus Corporate Edition provides scalable, cross-platform virus protection for workstations and network servers throughout the enterprise. Symantec System Center™ enables centralized configuration, deployment, policy management, and reporting*, and allows administrators to audit the network to determine which nodes are vulnerable to virus attacks. Administrators can manage client and server groups logically, and can create, deploy, and lock down security policies and settings to keep systems up-to-date and properly configured.

NAVEX™ and Digital Immune System™ technologies provide virus detection, analysis, and repairs via automated submission and response mechanisms. Expanded Threat Detection and Threat Categorization features detect unwanted spyware and adware, while a Threat Tracer feature helps administrators determine the source of blended threats spread through open file shares. Advanced behavior blocking prevents client systems from being used for malicious outbound activities, such as sending worms via email. A new Microsoft Installer results in self-healing capabilities and a 50% reduction in installation footprint. LiveUpdate™ technology allows administrators to configure automatic updates for virus definitions, including updates for definitions that are outdated.

Symantec VPN Sentry technology allows the administrator to ensure that mobile and remote systems connecting to corporate resources via VPN are compliant with security policies. The solution also ensures that machines not connected to the network can store and forward event data to administrators after reconnecting to the network.

*Graphical Reporting available via separate purchase

Installation Requirements

Hardware

- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)
- 32 MB of RAM

Software

- Windows 98/98 SE/Me
  Windows XP Professional/2000
  Professional/Server/Advanced Server/Server
  2003 Web/Standard/Enterprise/Datacenter
  Edition/NT 4.0 Workstation/Server/
  Terminal/Terminal Server Edition SP6a
- Internet Explorer 4.01 or later

Default Directory Structure - Program Folder

- C:\Program Files\Symantec AntiVirus

Default Directory Structure - Support Folders

- C:\Program Files\Symantec\LiveUpdate

- C:\Program Files\Common Files\Symantec Shared

Disk Space Requirements

- 55 MB of available hard-disk space

Key

This section is a guide to usage for the EAD document and lists sample items for illustration purposes. The items below represent typical program configuration items for a hypothetical drawing tool. Next to each option is 3 checkboxes. From left to right they represent Customer's choice (C), DCeS DSE's recommendation (R), and the program's default (D). All options marked with a ☑ in the left most column (Customer's choice) will be installed as part of the engineered solution. To the left of the choice checkboxes is a column indicating the support status of the individual options. The symbol ◎ represents an item that will be supported as part of a rate-based service. Items marked with a ○ will be supported on a time and materials basis only. Where a ◎ or a ○ is omitted, no attempt to interpret the support status is made. Most EAD's do not interpret the support status. For example…

Drawing Tools ← Major section

HDD Space: 125MB ← The amount of HDD space required as recommended by DCeS DSE. This entry is optional and may not appear on all EAD's

C R D ← Choice header

☑☑□Circle Tool ← Program Component

◎ ☑☑☑Square Tool ← Program Component

Comment [Ori1]: Alt-Y enters a Yes checkbox. Alt-N enters a No checkbox. Alt-S enters a rate-based service symbol. Alt-T enters a time and material symbol

**Turn off Show Markup to remove this box from printouts

In this example, the *Circle Tool* program component is not installed by default, DCeS DSE recommends the option, and the Customer is directing DCeS DSE to install the option. The *Circle Tool* will be supported on a time and materials or other basis as negotiated with Service Delivery. The *Square Tool* is a default installation option recommended by DCeS DSE and by the customer. It will be installed and supported under a rate-based service.

Installation Options

This section details the configuration that DCeS DSE will use to build the application.

Configuration Reference

This section describes the U.S. Army provided configuration documents that were referenced to configure SAV.

C R D

☑☑□ **Configure to Desktop Application STIG v2 rel 0, 26 July 2004**

SAV will be configured in accordance with the document listed above.

Client Administrator Only Options

General

Select the options you want for connected clients

C R D

Display

☑☑☑ Show Symantec AntiVirus icon on desktop (NOTE: desktop refers to the system tray)

Actions

☑☑☑ Display message when definitions are outdated

Warn after **<u>10</u>** days

Warning Message

“The virus definition file used is more than 10 days old. Updating to a new virus definition file will help catch the most recent viruses.”

Power Options

☑☑☑ Snooze scheduled scans when running on batteries

User disable/uninstall

☑☑☑ Lock the ability of users to unload Symantec AntiVirus Services

☑☑☑ Ask for password to allow uninstall of Symantec AntiVirus client; Password: *****

Scan network drive

☑□□ Ask for password to scan a mapped network drive; Password: *****

Client Realtime Protection Options

View

The following items have no configurable options: Realtime Scan Statistics, Scheduled Scans, Quarantine, Backup Items, and Repaired Items.

Scan

There is no current requirement.

Configure

♎ Represents a locked item. End users will “**<u>not</u>**” be able to modify this setting.

<u>File System Auto-Protect</u>

C R D

☑☑☑ **Enable Auto-Protect (Enabled)**

Advanced

Startup options

☑☑☑ System start

□□□ Symantec AntiVirus start

Changes requiring Auto-Protect reload

□□□ Wait until system restart

☑☑☑ Stop and reload Auto-Protect

Scan files when Auto-Protect will scan files that are:

□□□ Modified (scan on create)

☑☑☑♎ Accessed or modified (scan on create, open, move, copy, or run)

□□☑♎ Opened for backup (not applicable to Windows 9x or Netware)

☑☑☑ Preserver file times

☑☑☑ For Leave-Alone (Log only), delete infected files on creation.

File Cache

□□□ Disable file cache

☑☑☑ Use default file cache size

□□□ Custom file cache entries **0** (16 bytes/entry)

Automatic Enabler

☑☑☑♎ When Auto-Protect is disabled, enable after **5** minutes

Backup options

☑□☑♎ Back up file before attempting repair

Threat Tracer

☑☑☑ Enable Threat Tracer

☑☑☑ Resolve source computer IP address

☑☑☑ Poll for network sessions every **1000** milliseconds

☑☑☑ Client firewall auto blocks IP address of the source computer (NOTE: client firewall is not installed.)

Heuristics

☑☑☑♎ Enable Bloodhound ™ virus detection technology

Desired sensitivity level

□□□ Minimum level of protection

☑☑☑♎ Default level of protection

□□□ Maximum level of protection

Floppies

Floppy settings

☑☑☑♎ Check floppies for boot viruses upon access

When boot virus is found

☑☑☑♎ Clean a virus from boot record

□□□ Leave alone (log only)

System shutdown settings

□□□♎ Do not check floppies upon system shutdown

Files Types

☑☑☑♎ All types

□□□ Selected Extensions

386, ACM, ACV, ADT, AX, BAT, BIN, BTM, CLA, COM, CPL, CSC, CSH, DLL, DOC, DOT, DRV, EXE, HLP, HTA, HTM, HTML, HTT, INF, INI, JS, JSE, JTD, MDB, MP?, MSO, OBD, OBT, OCX, OV?, OVL, PIF, PL, PM, POT, PPS, PPT, RTF, SCR, SH, SHB, SHS, SMM, SYS, VBE, VBS, VSD, VSS, VST, VXD, WSF, WSH, XL?

☑☑☑ SmartScan

Macro Virus

1. Action

☑☑☑♎ Clean virus from file

□□□ Quarantine file

□□□ Delete infected file

□□□ Leave alone (log only)

2. If action fails

☑□☑♎ Quarantine file

☐☑☐ Delete infected file

☐☐☐ Leave alone (log only)

Non-Macro Virus

1. Action

☑☑☑♎ Clean virus from file

☐☐☐ Quarantine file

☐☐☐ Delete infected file

☐☐☐ Leave alone (log only)

2. If action fails

☑☐☑♎ Quarantine file

☐☑☐ Delete infected file

☐☐☐ Leave alone (log only)

☑☑☑♎ **Display message on infected computer**

Message

Scan type: [LoggedBy] Scan
Event: [Event]
[VirusName]
File: [PathAndFilename]
Location: [Location]
Computer: [Computer]
User: [User]
Action taken: [ActionTaken]
Date found: [DateFound]

☐☐☐♎ **Exclude selected files and folders**

Exclusions

Drive Types

☐☐☑♎ Network (NOTE: If checked, performance degrades when accessing servers)

☐☐☐ Floppy

☐☐☐ CD-ROM

<u>Internet E-mail Auto-Protect</u>

C R D

☑☑☑♎ **Enable Internet E-mail Auto-Protect**

Files Types

☑☑☑♎ All types

☐☐☐ Selected Extensions

386, ACM, ACV, ADT, AX, BAT, BIN, BTM, CLA, COM, CPL, CSC, CSH, DLL, DOC, DOT, DRV, EXE, HLP, HTA, HTM, HTML, HTT, INF, INI, JS, JSE, JTD, MDB, MP?, MSO, OBD, OBT, OCX, OV?, OVL, PIF, PL, PM, POT, PPS, PPT, RTF, SCR, SH, SHB, SHS, SMM, SYS, VBE, VBS, VSD, VSS, VST, VXD, WSF, WSH, XL?

☐☐☐ Select Types

Macro Virus

1. Action

☑☑☑♎ Clean virus from file

□□□ Quarantine file

□□□ Delete infected file

□□□ Leave alone (log only)

2. If action fails

☑□☑♎ Quarantine file

□☑□ Delete infected file

□□□ Leave alone (log only)

Non-Macro Virus

1. Action

☑☑☑♎ Clean virus from file

□□□ Quarantine file

□□□ Delete infected file

□□□ Leave alone (log only)

2. If action fails

☑□☑♎ Quarantine file

□☑□ Delete infected file

□□□ Leave alone (log only)

Outbound Worm Heuristics

1. Action

☑☑☑♎ Quarantine file

□□□ Delete infected file

□□□ Leave alone (log only)

2. If action fails

☑□☑♎ Delete infected file

□□□ Leave alone (log only)

Advanced – When scanning compressed files

☑☑☑♎ Scan files inside compressed files

If there is a compressed file within a compressed file

Expand **3** levels deep

Server port numbers

☑☑☑ Incoming server (POP3): **110**

☑☑☑ Outgoing server (SMTP): **25**

Heuristic detections

☑☑☑ Outbound Worm Heuristics

Progress notifications

☑☑☑ Display progress window when sending email

☑☑☑ Display tray icon

Notifications

☑☑☑♎ **Display message on infected computer**

Message

Scan type: [LoggedBy] Scan

Event: [Event]
[VirusName]
File: [PathAndFilename]
Location: [Location]
Computer: [Computer]
User: [User]
Action taken: [ActionTaken]
Date found: [DateFound]

☑☑☑♎ **Insert warning into email message**
Warning
☑☑□ Change the subject of the original message to:
Virus Found in message "[EmailSubject]"

☑☑☑ Message body
Symantec AntiVirus found a virus in an attachment from [EmailSender].

☑☑☑ Infection information (repeated for each infection)
Attachment: [OriginalAttachmentName]
[VirusName]
Action taken: [ActionTaken]
File status: [Status]

□□□♎ **Send e-mail to sender**
Compose
Subject:
Virus Found in message "[EmailSubject]"
Message body:
Symantec AntiVirus found a virus in an attachment you ([EmailSender]) sent to [EmailRecipientList].
Infection information (repeated for each infection)
Attachment: [OriginalAttachmentName]
[VirusName]
Action taken: [ActionTaken]
File status: [Status]

□□□♎ **Send e-mail to selected**
Address
Compose
Subject:
Virus Found in message "[EmailSubject]"
Message body:
Symantec AntiVirus found a virus in an attachment you ([EmailSender]) sent to [EmailRecipientList].
Infection information (repeated for each infection)
Attachment: [OriginalAttachmentName]
[VirusName]
Action taken: [ActionTaken]
File status: [Status]

Lotus Notes Auto-Protect

Not installed

<u>Microsoft Exchange Auto-Protect</u>

C R D

☑☑☑♎ **Enable**

Files Types

☑☑☑♎ All types

□□□ Selected Extensions

386, ACM, ACV, ADT, AX, BAT, BIN, BTM, CLA, COM, CPL, CSC, CSH, DLL, DOC, DOT, DRV, EXE, HLP, HTA, HTM, HTML, HTT, INF, INI, JS, JSE, JTD, MDB, MP?, MSO, OBD, OBT, OCX, OV?, OVL, PIF, PL, PM, POT, PPS, PPT, RTF, SCR, SH, SHB, SHS, SMM, SYS, VBE, VBS, VSD, VSS, VST, VXD, WSF, WSH, XL?

Macro Virus

1. Action

☑☑☑♎ Clean virus from file
□□□ Quarantine file
□□□ Delete infected file
□□□ Leave alone (log only)

2. If action fails

☑□☑♎ Quarantine file
□☑□ Delete infected file
□□□ Leave alone (log only)

Non-Macro Virus

1. Action

☑☑☑♎ Clean virus from file
□□□ Quarantine file
□□□ Delete infected file
□□□ Leave alone (log only)

2. If action fails

☑□☑♎ Quarantine file
□☑□ Delete infected file
□□□ Leave alone (log only)

Advanced – When scanning compressed files

☑☑☑♎ Scan files inside compressed files
If there is a compressed file within a compressed file
Expand <u>**3**</u> levels deep

Notifications

☑☑☑♎ **Display message on infected computer**

Message

Scan type: [LoggedBy] Scan
Event: [Event]
[VirusName]
File: [PathAndFilename]
Location: [Location]

Computer: [Computer]
User: [User]
Action taken: [ActionTaken]
Date found: [DateFound]

☑☑☑♎ **Insert warning into email message**
Warning

☑☑□ Change the subject of the original message to:
Virus Found in message "[EmailSubject]"

☑☑☑ Message body
Symantec AntiVirus found a virus in an attachment from [EmailSender].

☑☑☑ Infection information (repeated for each infection)
Attachment: [OriginalAttachmentName]
[VirusName]
Action taken: [ActionTaken]
File status: [Status]

□□□♎ **Send e-mail to sender**
Compose
Subject:
Virus Found in message "[EmailSubject]"
Message body:
Symantec AntiVirus found a virus in an attachment you ([EmailSender]) sent to [EmailRecipientList].
Infection information (repeated for each infection)
Attachment: [OriginalAttachmentName]
[VirusName]
Action taken: [ActionTaken]
File status: [Status]

□□□♎ **Send e-mail to selected**
Address
Compose
Subject:
Virus Found in message "[EmailSubject]"
Message body:
Symantec AntiVirus found a virus in an attachment you ([EmailSender]) sent to [EmailRecipientList].
Infection information (repeated for each infection)
Attachment: [OriginalAttachmentName]
[VirusName]
Action taken: [ActionTaken]
File status: [Status]

Quarantine Options

<u>Select options for Quarantine and Scan and Deliver</u>

C R D

□□□ Enable Quarantine or Scan and Deliver - There is no Quarantine server.

□□□ Allow Forwarding to Quarantine server
Server Name:
Port: **0**
Retry: **600**
Protocol: **IP** or **IPX**

□□□ Allow submissions via Scan and Deliver
□□□ Allow files to be resubmitted to SARC

When new virus definitions arrive:
☑☑□ Automatically repair and restore silently
□□□ Repair silently without restoring
□□□ Prompt user
□□□ Do nothing

Quarantine Purge Options…
☑☑☑ Enable automatic file purging
☑☑☑ Select the time period to purge the files <u>**7**</u> days

Repaired Items Purge Options…
☑☑☑ Enable automatic file purging
☑☑☑ Select the time period to purge the files <u>**7**</u> days

Backup Items Purge Options…
☑☑☑ Enable automatic file purging
☑☑☑ Select the time period to purge the files <u>**7**</u> days

Virus Definition Manager

<u>How Clients Retrieve Virus Definitions Updates</u>

C R D Options
□□□ **Update virus definitions from parent server (For Managed clients)**
□□□ Set client configuration from parent server **XX** minutes

☑☑□ **Schedule client for automatic product updates using LiveUpdate**
Frequency
☑☑□ Daily **11 am**
□□□ Weekly
□□□ Monthly
Advanced
Missed Events Options
☑☑□ Handle missed events within: **1** hour
□□□ _ days of scheduled time.
Randomization Options
☑☑□ Perform update within plus or minus

☑☑□ **60** minutes of the scheduled time

□□□ Randomize the day of the week within the interval

□□□ Beginning on **XX**, Ending **XX**

□□□ Randomize the day of month within plus or minus

□□□ 10 days of the scheduled date

☑☑□♎ Do not allow client to modify LiveUpdate schedule

□□□ Do not allow client to manually launch LiveUpdate

□□□ Enable continuous LiveUpdate

Options

□□□ LiveUpdate should check for new virus definitions every: **60** minutes (15-720)

□□□ Virus definitions should be updated when they are out of date by: **9** days (0-30)

□□□ Download product updates using LiveUpdate

Startup Scans

A scheduled scan will be implemented (see “Scheduled Scans”).

Custom Scans

There is no current requirement.

Scheduled Scans

C R D Select how often and when you want this scan to occur.

☑☑☑ Name: **Administrator Scan**

☑☑☑ Enable scan

	Frequency	**When**
□□□	Daily	
☑☑☑	Weekly	Every **Wednesday** at **12:00 PM**
□□□	Monthly	

☑☑☑ Advanced

Missed Event Options

☑☑☑ Handle missed events within **3** days of scheduled time

Files Types

☑☑☑ All types

□□□ Selected Extensions

386, ACM, ACV, ADT, AX, BAT, BIN, BTM, CLA, COM, CPL, CSC, CSH, DLL, DOC, DOT, DRV, EXE, HLP, HTA, HTM, HTML, HTT, INF, INI, JS, JSE, JTD, MDB, MP?, MSO, OBD, OBT, OCX, OV?, OVL, PIF, PL, PM, POT, PPS, PPT, RTF, SCR, SH, SHB, SHS, SMM, SYS, VBE, VBS, VSD, VSS, VST, VXD, WSF, WSH, XL?

Macro Virus

1. Action

☑☑☑ Clean virus from file

□□□ Quarantine file

□□□ Delete infected file

□□□ Leave alone (log only)

2. If action fails

☑□☑ Quarantine file

□☑□ Delete infected file

□□□ Leave alone (log only)

Non-Macro Virus

1. Action

☑☑☑ Clean virus from file

□□□ Quarantine file

□□□ Delete infected file

□□□ Leave alone (log only)

2. If action fails

☑□☑ Quarantine file

□☑□ Delete infected file

□□□ Leave alone (log only)

☑☑☑ **Display message on infected computer**

Message

Scan type: [LoggedBy] Scan
Event: [Event]
[VirusName]
File: [PathAndFilename]
Location: [Location]
Computer: [Computer]
User: [User]
Action taken: [ActionTaken]
Date found: [DateFound]

□□□ **Exclude selected files and folders**

Exclusions

Throttle Options

Scan priority 3 N 13
Priority when idle **Low**
Priority when not idle **Low**

□□□ Throttle NetWare Load

Advanced…

When scanning compressed files

☑☑☑ Scan files inside compressed files

If there is a compressed file within a compressed file

Expand **3** levels deep

Backup options

☑□☑ Back up file before attempting repair

Remote options

□☑☑ Show scan progress on computer being scanned
□☑□ Close scan progress when done
□☑□ Allow user to stop scan

Storage migration options (Win 2000 and later, consult your HSM vendor)
□□□ Skip offline files
□□□ Open files using backup semantics
☑☑☑ Skip offline and sparse files
□□□ Skip offline and sparse files with a reparse point
□□□ Scan resident portions of offline and sparse files
□□□ Scan all files, forcing demigration (fills drive)
□□□ Scan all files without forcing demigration (slow)
□□□ Scan all files recently touched without forcing demigration

Storage migration options (NetWare)
□□□ Scan NetWare compressed or migrated files

Look for Help

There are no configurable items.

Configure History

These options will affect the Virus History, Scan History, and Event Log.

Delete Histories
Select the time period to delete histories on the selected computer(s).
☑☑☑ Delete after **30 days** (days, months, years)

LiveUpdate Properties

□□☑ Symantec LiveUpdate server – LiveUpdate will obtain updates from an external DOD-CERT server

□□□ Internal LiveUpdate Server
Description
□□□ Name:
□□□ Location:
Login
□□□ Name:
□□□ Password:
Connection
□□□ URL or IP Address:
□□□ Type:
□□□ Subnet:
□□□ Subnet Mask:
□□□ Store passwords in encrypted form

☑☑☑ DOD-CERT LiveUpdate Site

☑☑☑ Access: ftp.cert.mil/pub/antivirus/NAV/signatures/LiveUpdate
☑☑☑ Name: ftp.cert.mil
☑☑☑ Type: FTP
☑☑☑ Login: anonymous
☑☑☑ Password: user.host.mil
☑☑☑ Hosts: 1
☑☑☑ Use Passive FTP Mode: 1

Client Roaming Options

There is no current requirement.

Client Event Forwarding

There is no current requirement.

Immediate Manual Scan

There is no current requirement.

Miscellaneous Options

There is no current requirement.

CAVEATS

- *Install*: Administrator privileges are required for installation.
- *Virus Updates*: A valid Internet connection is required to receive updated virus definitions when available from DOD-CERT LiveUpdate server.

Security Modifications

This section details security modifications to the desktop and documents items that were considered to pose a security risk by CSC personnel.

Rights Changes

This section details modifications to the rights for registry and file objects.

- NONE

Security Policy Changes

This section lists changes to the Local or Domain security policy required to support the application.

- NONE

Perceived Risks

The following section lists potential security risks as determined by the CSC Engineer.

Potential Impact	Risk
Low	Un-installation of software will require a password.